AMENDMENTS TO THE CLAIMS

1. (Currently amended) A computer-implemented method of analyzing security events, comprising:

receiving and processing security events from one or more security devices in a network, including grouping the security events into network sessions, each session having an identified source and destination;

causing display of a first graph on a display of a computer system, the first graph representing devices in the[[a]] network, the devices including the one or more security devices and non-security devices, the displayed first graph including one or more ~~a plurality of~~ individual device symbols and one or more ~~a plurality of~~ group device symbols, each individual device symbol representing one of the one or more a security devices ~~of the network~~ and each group device symbol representing a group of non-security devices of the network; ~~and~~

causing display~~, in conjunction with the graph, of security incident information including causing display, with respect to a group device symbol,~~ of a first security incident volume indicator on the display that indicates a number of network sessions whose source or destination is at any member of a group of non-security devices corresponding to a particular ~~the~~ group device symbol displayed on the display;

wherein causing display of the first security incident volume indicator includes causing the display to visually highlight the particular group device symbol in a manner that indicates the number network sessions whose source or destination is at any member of the group of non-security devices corresponding to the particular group device symbol.

2. (Currently amended) The computer-implemented method of claim 1, including:

upon user selection of the[[a]] particular group device symbol ~~for a group of non-security devices~~, causing display of a second level graph on the display of the computer system, the second level graph representing

(a) the members of the group of non-security devices corresponding to the particular group device symbol that are a source or destination of any of the network sessions of the number of network sessions indicated by the first security incident volume indicator, ~~in the group~~ and

(b) the security devices in association with the group of non-security devices corresponding to the particular group device symbol;

wherein[[,]] the displayed second level graph includes[[ing]] a plurality of non-security device symbols and a plurality of security device symbols, each non-security device symbol representing one non-security device from (a)~~in the group~~ and each security device symbol representing one security device from (b)~~in the group~~; ~~and~~

causing display~~, in conjunction with the second level graph, of security incident information, including causing display~~, with respect to at least one particular non-security device symbol from (a), of a second security incident volume indicator that indicates a number of network sessions whose source or destination is at the particular non-security device from (a).

3. (Currently amended) The computer-implemented method of claim 1, including

upon user command with respect to a user specified device symbol in the displayed first graph, causing display of data representing network sessions whose source or destination is at a device corresponding to the user specified device symbol.

4. (Currently amended) The computer-implemented method of claim 3, including in response to one or more user commands, selecting a network session from the displayed data, and defining a drop rule that comprises a set of network conditions corresponding to the selected network session;

wherein the processing of security events includes filtering out network sessions that satisfy the defined drop rule.

5. (Currently amended) The computer-implemented method of claim 3, wherein the data representing network sessions includes source and destination identifying information, event type information indicating one or more types of incidents corresponding to the network sessions, and security device information indicating one or more security devices that report security events in association with the network sessions.

6. (Currently amended) The computer-implemented method of claim 1, wherein the processing of security events includes identifying groups of network sessions that together satisfy a security incident identification rule in a group of predefined security incident identification rules, and identifying as rule firing network sessions each of the network sessions that is a member of any identified group of network sessions;

wherein each security incident volume indicator indicates a number of rule firing network sessions whose source or destination is at a device corresponding to the device symbol.

7. (Currently amended) The computer-implemented method of claim 6, wherein the processing of security events includes excluding from the rule firing network sessions any network session that satisfies any drop rule in a set of drop rules, each drop rule defining a respective set of conditions.

8-17. (Canceled)

18. (Currently amended) A network security events analysis system, comprising:

one or more central processing units for executing programs;

an interface for receiving security events; and

a network security event correlation engine executable by the one or more central processing units, the engine comprising:

instructions for receiving and processing security events from one or more security devices in a network, including grouping the security events into network sessions, each session having an identified source and destination;

instructions for display of a first graph on a display of a computer system, the first graph representing devices in the[[a]] network, the devices including the one or more security devices and non-security devices, the displayed first graph including one or more ~~a plurality of~~ individual device symbols and one or more ~~a plurality of~~ group device symbols, each individual device symbol representing one of the one or more a security devices ~~of the network~~ and each group device symbol representing a group of non-security devices of the network; ~~and~~

instructions for display~~, in conjunction with the graph, of security incident information including causing display, with respect to a group device symbol,~~ of a first security incident volume indicator on the display that indicates a number of network sessions whose source or destination is at any member of a group of non-security devices corresponding to a particular ~~the~~ group device symbol displayed on the display;

wherein the instructions for causing display of the first security incident volume indicator includes instructions for causing the display to visually highlight the particular group device symbol in a manner that indicates the number network sessions whose source or destination is at any member of the group of non-security devices corresponding to the particular group device symbol.

19. (Currently amended) The system of claim 18, including

instructions, responsive to user selection of the[[a]] particular group device symbol ~~for a group of non-security devices~~, for causing display of a second level graph on the display of the computer system, the second level graph representing

(a) the members of the group of non-security devices corresponding to the particular group device symbol that are a source or destination of any of the network sessions of the number of network sessions indicated by the first security incident volume indicator, ~~in the group~~ and

(b) the security devices in association with the group of non-security devices corresponding to the particular group device symbol;

wherein[[,]] the displayed second level graph includes[[ing]] a plurality of non-security device symbols and a plurality of security device symbols, each non-security device symbol representing one non-security device from (a)~~in the group~~ and each security device symbol representing one security device from (b)~~in the group~~; ~~and~~

instructions for causing display~~, in conjunction with the second level graph, of security incident information, including causing display~~, with respect to at least one particular non-security device symbol from (a), of a second security incident volume indicator that indicates a number of network sessions whose source or destination is at the particular non-security device from (a).

20. (Currently amended) The system of claim 18, including

instructions, responsive to a user command with respect to a user specified device symbol in the displayed first graph, for causing display of data representing network sessions whose source or destination is at a device corresponding to the user specified device symbol.

21. (Original) The system of claim 20, including instructions, responsive to one or more user commands, for selecting a network session from the displayed data, and defining a drop rule that comprises a set of network conditions corresponding to the selected network session; wherein the processing of security events includes filtering out network sessions that satisfy the defined drop rule.

22. (Original) The system of claim 20, wherein the data representing network sessions includes source and destination identifying information, event type information indicating one or more types of incidents corresponding to the network sessions, and security device information indicating one or more security devices that report security events in association with the network sessions.

23. (Previously Amended) The system of claim 18, wherein the processing of security events includes identifying groups of network sessions that together satisfy a security incident identification rule in a group of predefined security incident identification rules, and identifying as rule firing network sessions each of the network sessions that is a member of any identified group of network sessions; wherein each security incident volume indicator indicates a number of rule firing network sessions whose source or destination is at a device corresponding to the device symbol.

24. (Original) The system of claim 23, wherein the processing of security events includes excluding from the rule firing network sessions any network session that satisfies any drop rule in a set of drop rules, each drop rule defining a respective set of conditions.

25. (Currently amended) A computer program product for use in conjunction with a computer system, the computer program product comprising a computer readable storage

medium and a computer program mechanism embedded therein, the computer program mechanism comprising:

instructions for receiving and processing security events from one or more security devices in a network, including grouping the security events into network sessions, each session having an identified source and destination;

instructions for display of a first graph on a display of a computer system, the first graph representing devices in the[[a]] network, the devices including the one or more security devices and non-security devices, the displayed first graph including one or more ~~a plurality of~~ individual device symbols and one or more ~~a plurality of~~ group device symbols, each individual device symbol representing one of the one or more a security devices ~~of the network~~ and each group device symbol representing a group of non-security devices of the network; ~~and~~

instructions for display~~, in conjunction with the graph, of security incident information including causing display, with respect to a group device symbol,~~ of a first security incident volume indicator on the display that indicates a number of network sessions whose source or destination is at any member of a group of non-security devices corresponding to a particular ~~the~~ group device symbol displayed on the display;

wherein the instructions for causing display of the first security incident volume indicator includes instructions for causing the display to visually highlight the particular group device symbol in a manner that indicates the number network sessions whose source or destination is at any member of the group of non-security devices corresponding to the particular group device symbol.

26. (Currently amended) The computer program product of claim 25, including instructions, responsive to user selection of the[[a]] particular group device symbol ~~for a group of non-security devices~~, for causing display of a second level graph on the display of the computer system, the second level graph representing

(c) the members of the group of non-security devices corresponding to the particular group device symbol that are a source or destination of any of the network sessions of the number of network sessions indicated by the first security incident volume indicator, ~~in the group~~ and

(d) the security devices in association with the group of non-security devices corresponding to the particular group device symbol;

wherein[[,]] the displayed second level graph includes[[ing]] a plurality of non-security device symbols and a plurality of security device symbols, each non-security device symbol representing one non-security device from (a)~~in the group~~ and each security device symbol representing one security device from (b)~~in the group~~; ~~and~~

instructions for causing display~~, in conjunction with the second level graph, of security incident information, including causing display~~, with respect to at least one particular non-security device symbol from (a), of a second security incident volume indicator that indicates a number of network sessions whose source or destination is at the particular non-security device from (a).

27. (Currently amended) The computer program product of claim 25, including instructions, responsive to a user command with respect to a user specified device symbol in the displayed first graph, for causing display of data representing network sessions whose source or destination is at a device corresponding to the user specified device symbol.

28. (Original) The computer program product of claim 27, including instructions, responsive to one or more user commands, for selecting a network session from the displayed data, and defining a drop rule that comprises a set of network conditions corresponding to the selected network session; wherein the processing of security events includes filtering out network sessions that satisfy the defined drop rule.

29. (Original) The computer program product of claim 27, wherein the data representing network sessions includes source and destination identifying information, event type information indicating one or more types of incidents corresponding to the network sessions, and security device information indicating one or more security devices that report security events in association with the network sessions.

30. (Previously Amended) The computer program product of claim 25, wherein the processing of security events includes identifying groups of network sessions that together satisfy

a security incident identification rule in a group of predefined security incident identification rules, and identifying as rule firing network sessions each of the network sessions that is a member of any identified group of network sessions; wherein each security incident volume indicator indicates a number of rule firing network sessions whose source or destination is at a device corresponding to the device symbol.

31. (Original) The computer program product of claim 30, wherein the processing of security events includes excluding from the rule firing network sessions any network session that satisfies any drop rule in a set of drop rules, each drop rule defining a respective set of conditions.

32. (New) The computer-implemented method of claim 1, further comprising:

identifying one or more of the network sessions as satisfying at least one predetermined security event correlation rule, wherein the at least one predetermined security event correlation rule specifies criteria of a set of one or more security events that indicate a security incident;

wherein said number of network sessions whose source or destination is at any member of a group of non-security devices corresponding to the particular group device symbol is the number of identified network sessions whose source or destination is at any member of a group of non-security devices corresponding to the particular group device symbol displayed on the display.

33. (New) The computer-implemented method of claim 1, wherein causing the display to visually highlight the particular group device symbol in a manner that indicates the number network sessions whose source or destination is at any member of the group of non-security devices corresponding to the particular group device symbol comprises causing display of a separate security incident volume indicator substantially adjacent to the particular group device symbol for each one of the number of network sessions whose source or destination is at any member of the group of non-security devices corresponding to the particular group device symbol.

34. (New) The computer-implemented method of claim 1, wherein causing the display to visually highlight the particular group device symbol in a manner that indicates the number

network sessions whose source or destination is at any member of the group of non-security devices corresponding to the particular group device symbol comprises causing a change in the appearance of the particular group device symbol to indicate the number network sessions whose source or destination is at any member of the group of non-security devices corresponding to the particular group device symbol.

35. (New) The system of claim 18, further comprising:

instructions for identifying one or more of the network sessions as satisfying at least one predetermined security event correlation rule, wherein the at least one predetermined security event correlation rule specifies criteria of a set of one or more security events that indicate a security incident;

wherein said number of network sessions whose source or destination is at any member of a group of non-security devices corresponding to the particular_group device symbol is the number of identified network sessions whose source or destination is at any member of a group of non-security devices corresponding to the particular group device symbol displayed on the display.

36. (New) The system of claim 18, wherein the instructions for causing the display to visually highlight the particular group device symbol in a manner that indicates the number network sessions whose source or destination is at any member of the group of non-security devices corresponding to the particular group device symbol comprises instructions for causing display of a separate security incident volume indicator substantially adjacent to the particular group device symbol for each one of the number of network sessions whose source or destination is at any member of the group of non-security devices corresponding to the particular group device symbol.

37. (New) The system of claim 18, wherein the instructions for causing the display to visually highlight the particular group device symbol in a manner that indicates the number network sessions whose source or destination is at any member of the group of non-security devices corresponding to the particular group device symbol comprise instructions for causing a change in the appearance of the particular group device symbol to indicate the number network

sessions whose source or destination is at any member of the group of non-security devices corresponding to the particular group device symbol.

38. (New) The computer program product of claim 25, further comprising instructions for identifying one or more of the network sessions as satisfying at least one predetermined security event correlation rule, wherein the at least one predetermined security event correlation rule specifies criteria of a set of one or more security events that indicate a security incident; wherein said number of network sessions whose source or destination is at any member of a group of non-security devices corresponding to the particular_group device symbol is the number of identified network sessions whose source or destination is at any member of a group of non-security devices corresponding to the particular group device symbol displayed on the display.

39. (New) The computer program product of claim 25, wherein the instructions for causing the display to visually highlight the particular group device symbol in a manner that indicates the number network sessions whose source or destination is at any member of the group of non-security devices corresponding to the particular group device symbol comprise instructions for causing display of a separate security incident volume indicator substantially adjacent to the particular group device symbol for each one of the number of network sessions whose source or destination is at any member of the group of non-security devices corresponding to the particular group device symbol.

40. (New) The computer program product of claim 25, wherein the instructions for causing the display to visually highlight the particular group device symbol in a manner that indicates the number network sessions whose source or destination is at any member of the group of non-security devices corresponding to the particular group device symbol comprise instructions for causing a change in the appearance of the particular group device symbol to indicate the number network sessions whose source or destination is at any member of the group of non-security devices corresponding to the particular group device symbol.